(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 43 42 641 A 1**

(51) Int. Cl.[6]:
G 07 C 9/00
H 04 L 9/32
B 60 R 25/00
// E05B 49/00

(21) Aktenzeichen: P 43 42 641.7
(22) Anmeldetag: 14. 12. 83
(43) Offenlegungstag: 22. 6. 95

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Reiner, Robert, Dipl.-Ing., 82008 Unterhaching, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Authentifikation zwischen einem mobilen Datenträger und einer stationären Datenstation

(57) Das erfindungsgemäße Verfahren zur Authentifikation zwischen einem mobilen Datenträger und einer stationären Datenstation erfolgt mittels eines Kryptoalgorithmus. Der mobile Datenträger weist einen ersten schützbaren Speicherbereich auf, indem bei Herstellung des mobilen Datenträgers eine Zufallszahl gespeichert wird. In einem zweiten geschützten Speicherbereich wird ein dem mobilen Datenträger zugehöriger Geheimcode eingeschrieben. Die stationäre Datenstation speichert sowohl Zufallszahl sowie individuellen Geheimcode eines jeden zugehörigen mobilen Datenträgers. Die Datenstation erkennt bei erstmaliger Benutzung eines neuen zulässigen Datenträgers diesen durch die gespeicherte Zufallszahl. Die Zulässigkeit des neuen Datenträgers wird mittels des Kryptoalgorithmus erkannt. Daraufhin wird ein neuer Geheimcode generiert und im mobilen Datenträger abgespeichert.

DE 43 42 641 A 1

DE 43 42 641 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Authentifkation zwischen einem mobilen Datenträger und einer stationären Datenstation gemäß dem Oberbegriff des Anspruchs 1.

Ein derartiges Verfahren findet z. B. bei elektronischen Schlüssel-Schloßsystemen Anwendung. Insbesondere kann ein derartiges Verfahren bei einer Kfz-Wegfahrsperre zum Einsatz kommen, bei der der mobile Datenträger sich innerhalb des Zündschlüssels befindet und die stationäre Datenstation z. B. in der Motorsteuerung untergebracht ist. Die Versorgung des Schlüssels mit der Betriebsleistung und Daten kann z. B. auf induktivem Weg erfolgen. Dazu wird um das Zündschloß eine Spule angebracht, die mit einem Kondensator einen Resonanzkreis bildet. Das Schloß besteht aus einem Schließzylinder, aus einer Bronzelegierung und einer Halterung aus einem Druckgußmetall. Der Schlüssel enthält ebenfalls eine Spule, die Teil eines Resonanzkreises ist, der auf den Resonanzkreis des Schlosses abgestimmt ist.

Die Authentifikation selbst kann bei derartigen Systemen über bekannte Kryptoalgorithmen, wie sie z. B. bei Chipkarten verwendet werden, erfolgen.

Insbesondere im Kfz-Bereich sind jedoch die Sicherheitsforderungen, besonders die der Kfz-Versicherer, sehr hoch.

So gilt es zu verhindern, daß nichtberechtigte Personen in der Lage sind, zulässige Schlüssel nachzubilden, indem sie z. B. den Schlüssel dekodieren oder den Datenverkehr zwischen Schlüssel und Schloß "abhören", um so zu den gewünschten geheimen Daten zu gelangen.

Aufgabe der vorliegenden Erfindung ist es ein Verfahren zur Authentifikation zwischen einem mobilen Datenträger und einer stationären Datenstation anzugeben, das einem hohen Sicherheitsstandard entspricht.

Diese Aufgabe wird durch den kennzeichnenden Teil des Anspruchs 1 gelöst. Weiterbildungen sind Kennzeichen der Unteransprüche.

Das erfindungsgemäße Verfahren findet Anwendung in einem System bestehend aus Schlüssel und Schloß. Der Schlüssel enthält einen mobilen Datenträger, der mit einer stationären Datenstation, dem Schloß, Daten austauschen kann. Ebenso versorgt die stationäre Datenstation den mobilen Datenträger mit einer Versorgungsspannung. Beides Energie und Datenübertragung kann z. B. auf induktiven Weg erfolgen.

Der mobile Datenträger kann eine Vielzahl von geschützten und nicht geschützten Speicherbereichen aufweisen. Der Aufbau des Speichers des mobilen Datenträgers kann dabei beispielsweise folgendermaßen aussehen:

In einem ersten ungeschützten Speicherbereich kann eine Identifikationsnummer, z. B. vom Kfz-Hersteller, eingeschrieben werden. Dieser dient später der Unterscheidung von z. B. n verschiedenen Schlüssel pro Fahrzeug und/oder anderen Zwecken nach Belieben des Fahrzeugherstellers.

Ein zweiter Speicherbereich enthält eine Zufallszahl, die gegenüber Schreiben geschützt ist. Diese dient dazu, den Schlüsselrohling im Fall der Verwendung als Ersatzschlüssel für das elektronische Schloß vom Originalschlüssel unterscheidbar zu machen. Diese Zufallszahl wird bereits beim Halbleiterhersteller programmiert und ist gegenüber Schreiben geschützt, kann also weder vom Kfz-Hersteller noch von berechtigten bzw. unberechtigten Personen überschrieben werden.

In einem weiteren Speicherbereich kann ein Frequenzabgleichwert für das Schlüsselmodul abgespeichert werden. Dieses wird erst beim Endtest beschrieben und evtl. gegen Überschreiben geschützt werden, wenn dies als vorteilhaft angesehen wird. In einem weiteren Speicherbereich kann das Teilerverhältnis zwischen Trägerfrequenz und Baudrahte abgespeichert werden. Dieser Bereich kann entweder beim Halbleiterhersteller oder beim Kfz-Hersteller beschrieben werden.

Vom Chip aus muß sichergestellt sein, daß das zusammengebaute Modul, d. h. der Schlüssel mit dem darin integrierten mobilen Datenträger, mit einer definierten Baudrate angesprochen werden kann. Das kann beispielsweise dadurch geschehen, daß entweder von der Scheibenherstellung her ein bestimmter Wert in den Speicherbereich für das Teilerverhältnis abgespeichert worden ist und diesem Wert, der z. B. OOH oder FFH sein kann, schaltungsmäßig ein geeignetes Verhältnis zugeordnet ist, oder daß bei der Scheibenmessung z. B. über extra Pads dieser Wert eingeschrieben wird. Bei der Endmessung des Moduls wird dann der für den Kfz-Hersteller notwendige Wert eingeschrieben und kann dann auch gegenüber Schreiben geschützt werden, wenn dies als vorteilhaft angesehen wird.

Ein weiterer Speicherbereich ist vorgesehen, indem später der Geheimcode gespeichert wird. Dieser Bereich ist derart ausgestattet, daß er nicht von außen lesbar ist und nur schreibbar nachdem eine erfolgreiche Authentifikation stattgefunden hat. Bei der Auslieferung z. B. an den Kfz-Hersteller müssen sie einen Wert enthalten, der dem Kunden bekannt ist, weil nur mit Kenntnis dieses Wertes ein Schreiben in dem Bereich möglich ist. Ein Lesen ist wie bereits erwähnt nie möglich. Dies kann dadurch geschehen, daß entweder von der Scheibenherstellung her ein bestimmter Wert in den Bytes des geheimen Speicherbereichs vorhanden ist, z. B. OOH oder FFH, oder daß bei der Scheibenmessung z. B. über extra Pads dieser Wert eingeschrieben wird.

Eine weitere Möglichkeit wäre die einzelnen Chips mit einem individuell vereinbarten Transportcode für eine Lieferung zu schützen. Wenn die Lieferung verloren geht, kann der unbekannte Finder mit den Modulen bzw. Rohschlüsseln nichts anfangen, da der Inhalt des geheimen Speicherbereichs nicht bekannt ist.

Da Schlüssel und Schloß, bzw. mobiler Datenträger und stationäre Datenstation erst beim Kunden, z. B. dem Kfz-Hersteller, zusammenkommen, muß dieser die einzelnen Schlüssel dem jeweiligen elektronischen Schloß zuordnen und initialisieren.

So muß z. B. in den ersten Speicherbereich eingeschrieben werden, um welchen Fahrzeugschlüssel es sich handelt. Ebenso, müssen die Bereiche für das Verhältnis zwischen Trägerfrequenz und Baudrate eingeschrieben werden. Schließlich folgt der dem jeweiligen Schloß zugehörige individuelle Geheimcode für den Schlüssel.

Im elektronischen Schloß, d. h. der stationären Datenstation, muß für jeden zugeordneten Schlüssel der jeweilige Datensatz des Schlüssels gespeichert werden. Dieser Datensatz besteht aus der Identifikationsnummer, der in dem geschützten Speicherbereich abgelegten Zufallszahl sowie dem individuellen Geheimcode in dem nicht lesbaren Speicherbereich.

Für nicht ausgelieferte Schlüssel können auch diese Daten eingeschrieben werden, als würden diese Schlüs-

sel existieren. Dann können später zusätzliche Schlüssel bestellt werden, als wären sie die Ersatzschlüssel.

Außerdem muß der Kfz-Hersteller diese Inhalte dokumentieren, um später die Informationen für Ersatzschlüssel oder den Ersatz der Steuergeräte, die das elektronische Schloß, also die stationäre Datenstation, enthalten, zu ermöglichen.

Die eigentliche Authentifikation kann über bekannte Kryptoalgorithmen erfolgen. Hierzu kann z. B. eine von der stationären Datenstation an den mobilen Datenträger gesendete Zufallszahl durch einen Kryptoalgorithmus im mobilen Datenträger mittels des Geheimcodes verschlüsselt werden. Das Ergebnis dieser Berechnung kann zusammen mit dem Identifikationscode des Schlüssels, der aus der Identifikationsnummer, also der Schlüsselnummer, und der Zufallszahl besteht, an die stationäre Datenstation übermittelt werden. Diese berechnet mit dem gleichen Kryptoalgorithmus und dem Geheimcode das Ergebnis und vergleicht dieses mit dem vom mobilen Datenträger übermittelten. Es wird also nie der Geheimcode selbst übermittelt und kann somit auch nicht von einer unberechtigten Person abgehört werden. Stimmen beide miteinander überein, so handelt es sich um einen gültigen Schlüssel bzw. mobilen Datenträger.

In einem weiteren Schritt kann nun anhand der Schlüsselnummer und der Zufallszahl überprüft werden, ob der Schlüssel bei der Initialisierung der stationären Datenstation abgespeichert wurde. Ist dies der Fall, so wird das Schloß freigegeben, und die daran angeschlossene Wegfahrsperre deaktiviert.

Wenn ein Schlüssel verloren, gestohlen oder zerstört würde, kann man einen Ersatzschlüssel anfertigen lassen. Dabei wird erfindungsgemäß automatisch der alte Schlüssel ungültig. Der Schutz gegen Diebstahl ist daher auch im Fall eines gestohlenen Schlüssels wieder herzustellen.

Der Kunde meldet sich in einer Ersatzschlüsselwerkstatt und weist sich dort aus. Er gibt an, welchen Schlüssel er verloren hat, wenn er das weiß, ansonsten wird eine Schlüsselnummer angenommen. Die Ersatzschlüsselwerkstatt fragt bei der Ersatzschlüsselzentrale des Kraftfahrzeugherstellers nach dem Geheimnis des verlorenen Schlüssels. Dieser Datenverkehr muß geschützt abgewickelt werden. Die Werkstatt fräst den Bart des Schlüssels und programmiert die Schlüsselnummer im ungeschützten Speicherbereich, sowie den alten vom Kfz-Hersteller übermittelten Geheimcode in den entsprechenden Speicherzellen des mobilen Datenträgers.

Der Kunde erhält den Schlüssel und begibt zu seinem Fahrzeug. Dort wendet er den Ersatzschlüssel an. Das Schloß, d. h. die stationäre Datenstation, stellt nun fest, daß der Schlüssel den richtigen Geheimcode enthält, er also berechtigt ist, daß aber die im geschützten Speicherbereich abgespeicherte Zufallszahl nicht in seinem Speicherbereich abgespeichert ist, da es sich um einen neuen Schlüssel mit einer neuen bisher nicht bekannten Zufallszahl handelt. Daraufhin generiert und programmiert das elektronische Schloß einen neuen Geheimcode in den Schlüssel. Außerdem macht die stationäre Datenstation zunächst alle anderen Schlüssel ungültig. Dies ist der einzige Moment, wo der Geheimcode abgehört werden könnte. Jedoch ist praktisch auszuschließen, daß eine nicht berechtigte Person in diesem Moment Zugang zum Schlüssel-Schloß-System hat. Vorteil dieses Verfahrens ist, daß die schlüsselherstellende Werkstatt nun den Geheimcode nicht mehr weiß und somit auch hier keine unberechtigten Personen einen weiteren Ersatzschlüssel anfertigen können.

Über die in der stationären Datenstation enthaltene Software kann der Kraftfahrzeughersteller festlegen, wie der neue Geheimcode generiert wird. Hierzu bestehen mehrere Möglichkeiten.

1. Durch einen echten Zufallsgenerator. Niemand kann danach wissen, wie der neue Geheimcode lautet. Vorteil dieses Verfahrens ist eine sehr hohe Sicherheit. Der Nachteil dieses Verfahrens besteht darin, daß nur ein Ersatzschlüssel gefertigt werden kann, da ab Verwendung des Ersatzschlüssels der Geheimcode niemanden mehr bekannt ist.
2. Durch einen Algorithmus, der z. B. aus dem alten Geheimcode und der alten Identifikation des verlorenen Schlüssels den neuen Geheimcode generiert. Der Vorteil liegt darin, daß der Kraftfahrzeughersteller auch das neue Geheimnis berechnen kann und man für einen evtl. verlorenen Ersatzschlüssel einen neuen Ersatzschlüssel herstellen kann. Der Nachteil besteht darin, daß die Sicherheit theoretisch etwas geringer als bei der ersten Variante ist, weil der Algorithmus zur Geheimcodegenerierung bekannt werden könnte. Jedoch reicht im Normalfall die Kenntnis des alten Geheimcodes auch dann nicht aus, weil die im geschützten Speicherbereich gespeicherte Zufallszahl des verlorenen Schlüssels nicht einmal dem Hersteller des Ersatzschlüssels bekannt ist. Dem Finder des alten Schlüssels sind zwar die Zufallszahl jedoch nicht der Geheimcode bekannt.

Ein Diebstahl eines Kraftfahrzeugs, das mit einem erfindungsgemäßen Schlüssel-Schloßsystem ausgestattet ist, wäre nur denkbar, wenn ein Vertrauter der Ersatzschlüsselwerkstatt den Schlüssel stiehlt, und damit Kenntnis der alten Identifikationsnummer erlangt. Außerdem müßte der Ersatzschlüssel tatsächlich in dieser Werkstatt hergestellt werden und die Programmieranlage angezapft werden, damit der alte Geheimcode bekannt wird. Schließlich müßte der Algorithmus zur Geheimcodegenerierung bekannt sein, nur in diesem Fall könnte die Werkstatt dann einen Schlüssel anfertigen, der von der stationären Datenstation, dem Schloß, als gültiger Ersatzschlüssel erkannt würde. Dieser Fall läßt sich ausschließen, wenn das elektronische Schloß eine nicht auslesbare und individuelle Geheimzahl enthält, die im Algorithmus zur Erzeugung des neuen Geheimcodes verwendet wird.

Da das elektronische Schloß bei diesem Verfahren alle anderen Schlüssel zunächst sperrt, kann in einer Weiterbildung eine Möglichkeit geschaffen werden, diese wieder zu entsperren. Hierzu muß das Kraftfahrzeug mit einem gültigen Schlüssel, z. B. dem neuen Ersatzschlüssel, eingeschaltet werden. Nach dem Abziehen des gültigen Schlüssels kann dann innerhalb einer kurzen Zeit ein anderer zum Kraftfahrzeug gehöriger Schlüssel eingesteckt werden, der dann entsperrt wird, wenn er elektronisch paßt. Auf diese Weise können wieder alle übrig gebliebenen Schlüssel gültig gemacht werden. Falls der Ersatzschlüssel aus Unkenntnis auf die Schlüsselnummer im ersten ungeschützten Speicherbereich, eine zuhause liegenden Schlüssels programmiert wurde, bleibt dieser Schlüssel allerdings nutzlos wie der eventuell verlorene Schlüssel.

In einem weiteren Fall sei angenommen, daß die stationäre Datenstation, d. h. das elektronische Schloß, sich in der Motorsteuerung befindet, und diese im Repara-

turfall ausgewechselt werden muß.

Die Werkstatt muß den Geheimcode aller Schlüssel in das elektronische Schloß der Ersatzmotorsteuerung programmieren. Das ist ohne weiters möglich, weil sich die Geheimcodes jederzeit einprogrammieren, aber nie auslesen lassen. Die Werkstatt erfährt die Geheimcodes von der Ersatzschlüsselzentrale des Kraftfahrzeugherstellers.

Bei der ersten Anwendung der vorhandenen Kraftfahrzeugschlüssel werden diese wie Ersatzschlüssel behandelt, da die Werkstatt die Zufallszahl der einzelnen Schlüssel nicht kennen muß und diese auch nicht im neuen elektronischen Schloß einspeichern kann. Daraufhin werden diese vorhandenen Kraftfahrzeugschlüssel von dem neuen elektronischen Schloß wie Ersatzschlüssel behandelt und es werden neue Geheimnisse von dem neuen elektronischen Schloß generiert und in die Schlüssel geschrieben. Damit werden die neuen Geheimcodes der Werkstatt unbekannt. Dieses Verfahren funktioniert vor allem bei der zweiten Variante der Generierung neuer Geheimcodes, wie oben beschrieben, weil sonst die Beschaffung von Ersatzschlüsseln verhindert wäre.

Es bleibt das geringe Risiko, daß eine auf Betrug ausgelegte Werkstatt sowohl Kenntnis der Identifikationsnummer der Schlüssel wie deren alten Geheimcodes hat und sich bei Kenntnis des Algorithmus zur Generierung der neuen Geheimcodes somit diese errechnen kann. Sie könnte nur dann Schlüssel anfertigen, die vom Kraftfahrzeug als gültige Ersatzschlüssel anerkennt würden. Dieser Fall ist jedoch praktisch auszuschließen.

Patentansprüche

1. Verfahren zur Authentifikation zwischen einem mobilen Datenträger und einer stationären Datenstation, wobei der mobile Datenträger geschützte und nicht geschützte Speicherbereiche sowie Mittel zur Datenübertragung aufweist, die Authentifikation des mobilen Datenträgers bzw. der stationären Datenstation mittels eines Kryptoalgorithmus und einer im mobilen Datenträger gespeicherten Geheimcode erfolgt, **dadurch gekennzeichnet,** daß
   - in einem ersten schützbaren Speicherbereich des mobilen Datenträgers eine individuelle Zahl, z. B. Zufallszahl gespeichert und gegen Überschreiben geschützt wird,
   - in einem zweiten nicht lesbaren und geschützt schreibbaren Speicherbereich ein der Authentifikation zugehöriger Geheimcode eingeschrieben wird,
   - die stationäre Datenstation die individuelle Zufallszahl und den individuellen Geheimcode eines jeden zugehörigen mobilen Datenträgers gespeichert hat,
   - die Datenstation bei erstmaliger Benutzung eines neuen mobilen Datenträgers, diesen durch die im mobilen Datenträger gespeicherte individuelle Zufallszahl als neu erkennt und über den Kryptoalgorithmus die Echtheit des mobilen Datenträgers feststellt und daraufhin einen neuen Geheimcode generiert und diesen im mobilen Datenträger in dem nicht lesbaren und geschützt schreibbaren Speicherbereich abspeichert.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der neue Geheimcode durch einen Zufallsgenerator erzeugt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der neue Geheimcode durch einen Algorithmus mittels des alten Geheimcodes und/oder der Zufallszahl erzeugt wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der mobile Datenträger einen ungeschützten oder schützbaren Speicherbereich aufweist, indem ein Code zur individuellen Unterscheidung des mobilen Datenträgertyps gespeichert wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
   - daß bei Erkennen eines neuen bisher nicht gespeicherten mobilen Datenträgers, alle bisherigen mobilen Datenträger für die Authentifikation gesperrt werden,
   - während einer bestimmten vorgebbaren Zeit nach der Authentifikation des neuen Datenträgers, die alten Datenträger durch eine Authentifikation der jeweiligen mobilen Datenträger wieder in der stationären Datenstation entsperrt werden.

6. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß das Schloß eine nicht aus lesbare und nicht überschreibbare individuelle Geheimzahl enthält, die im Algorithmus zur Erzeugung des neuen Geheimcodes verwendet wird.